

Anonym-surfen

In diesem Tutorial wollen wir uns mit den Möglichkeiten des anonymen Surfens beschäftigen. Dabei zuerst einmal die Erläuterung, was unter dem Begriff "**anonym surfen**" überhaupt verstanden wird.

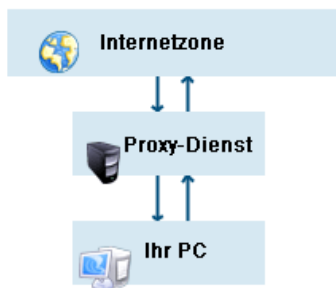
Der Begriff "**anonym surfen**" beschreibt die Zielsetzung, seine persönlichen Daten, die einen Rückschluss zu Ihnen zulassen wie etwa Ihre IP-Adresse so zu verschleiern, dass es unmöglich ist diese zurück zu verfolgen.

Also ist unter dem Begriff anonym surfen ein Netzdienst zu verstehen, der es Internetnutzern ermöglicht unerkannt Webseiten zu besuchen.

Dabei werden Webseiten nicht direkt vom Computer des Surfers aus geladen, sondern über einen Proxy eines Servers des jeweiligen Anbieters.

Der Vorteil für den User liegt darin, dass zu keiner Zeit sein Computer direkt mit der Webseite, die er besucht verbunden ist, sondern immer der Anbieterserver 'dazwischengeschaltet' ist.

Anonym surfen beinhaltet also Sicherheit vor Datenspionen, da diese nicht direkt an Sie herankommen können und sollen.



Diese Visualisierung soll verdeutlichen, wie diese Technik im groben funktioniert.

Ihr Computer ist mit dem Proxy-Server verbunden. Dieser wiederum ruft die von Ihnen gewünschten Webseiten auf.

Sie können dann also diese Webseiten über den Dazwischengeschalteten Proxy-Dienst betrachten.

Doch auch diese Art des Surfens ist nicht frei von Gefahren. Dazu allerdings mehr in einem anderen Unterpunkt.

anonym-surfen-Grundlagen

In den Grundlagen zum Thema 'anonym surfen' müssen wir ein wenig ausholen um Ihnen mehrere Dinge zu verdeutlichen. Da wären:

- wie funktioniert das Surfen im Internet?

Ihr **Internet-Zugangsprovider**

- Was spielen **IP's** für eine Rolle und was ist das überhaupt?

Das Internet setzt sich aus sehr vielen zusammengesetzten Netzwerken zusammen, die allesamt über verschiedenste IP's (IP = Internet Protocol) angesteuert werden können. Wenn Sie sich zu Hause oder an Ihrem Arbeitsplatz mit dem Internet verbinden, dann erhalten Sie von Ihrem Zugangsprovider eine IP. Diese IP ist ähnlich wie eine Telefonnummer zu betrachten.

Es gibt variable IP's und 'feste' IP's. Wenn Sie bei Ihrem Provider eine feste IP gemietet haben, dann ist es beispielsweise möglich, Ihren eigenen Computer auch als WebServer fungieren zu lassen.

Variable IP's erhalten Sie aber in der Regel von Ihrem Provider, bei 'normaler' Kontaktaufnahme mit dem Internet.

Technisch müssen Sie sich das in etwa so vorstellen:

- Anfrage bei Ihrem Provider
- IP Zuweisung des Providers und Netzwerkverbindung über ebendiesen
- Rückmeldung Ihres Providers an Ihren Computer mit der Verbindungsherstellung

Nun sind Sie online. Für den Tutorial-Bereich "anonym surfen" sollte Ihnen schon anhand dieser kurzen Einführung klar sein, dass Sie immer und zu jeder Zeit, die Sie mit dem Internet verbunden sind, auch immer anhand dieser IP über Ihren Provider identifiziert werden können.

Da Ihr Provider diese IP und die Verbindungsdauer abspeichert, ist es diesem später möglich Ihnen detaillierte Rechnungen über Einwahlen und Dauer zukommen zu lassen.

Merke: Sie sind also immer und zu jeder Zeit anhand Ihrer virtuellen Telefonnummer (IP) zurück verfolgbar.

- nun gehe ich mit dieser, meiner IP, zu einer Whois-Abfrage zum Beispiel diese:

<http://www.whois-search.com>

Sie erhalten dann sofort Auskunft in dieser Form und kann schon sehen, dass ich über "HanseNet Telekommunikation" in Hamburg gerade online bin.

Nun ist es zum Beispiel für Ermittlungsbehörden kein Problem mehr mit Ihrer ermittelten IP und Ihren Provider auch direkt an Sie heran zu kommen.

Webseiten-Aufrufen

So, wie Sie von Ihrem Provider eine IP bei jedem Internet Verbindungsaufbau eine zugewiesen bekommen, so gibt es auch noch die 'festen' IP-Adressen.

Hier wollen wir uns allerdings ausschließlich mit Webseiteninhalten und deren Aufrufs beschäftigen.

Technisch ist es so, dass jedem Webserver eine feste IP zugewiesen ist. Unter dieser 'Telefonnummer' ist immer dieser eine bestimmte Server "am Apparat".

Nun ist es so, dass sich Keiner diese auf den ersten Blick komisch anhäufenden Zahlenberg merken kann. Es wurden also für den Menschen leichter zu merkende Variablen geschaffen.

Kurz: die Geburtsstunde der Domains

Auf solch einem Webserver ist aber in der Regel nicht nur eine einzige Domain beheimatet. Der Webhoster schaltet via eines DNS (Domain Name Server) Eintrages bis zu mehreren Hundert und zum Teil sogar bis zu mehreren tausend Domains auf so einen Server.

Hier mal ein Beispiel eines sehr informativen Counterservices von der Firma Etracker visualisiert:

13:28:16.7900 17.08.2005	84.135.249.163 -.dip.t-dialin.net (dialup) Browse http://www.google.de/search?... Google Deutschland: Virenschutz 06	WinXP IE 6.0	1024 x 768 True Color (32 bit) Germany Bielefeld	00:00:00 1 Seite Tracking
13:28:12.1300 17.08.2005	172.177.233.117 -.ipt.aol.com (dialup) Browse http://www.crazysms.sevens-ser...	WinXP IE 6.0	1024 x 768 True Color (32 bit) Germany Aol	00:00:00 1 Seite Tracking
13:27:15.8900 17.08.2005	194.208.139.133 -.TELE.NET (cable) Browse http://www.google.at/search?... Google Österreich: testberichte antivirus	WinXP IE 6.0	1024 x 768 True Color (32 bit) Austria Feldkirch	00:00:25 3 Seiten Tracking
13:24:21.7800 17.08.2005	84.191.79.77 -.dip.t-dialin.net (dialup) Browse http://www.google.de/search?... Google Deutschland: test antivir spyware	WinXP IE 6.0	1024 x 768 True Color (32 bit) Germany Berlin	00:00:23 2 Seiten Tracking
13:23:47.7400 17.08.2005	80.184.176.246 -.d.pppool.de (broadband) Browse http://www.google.de/search?... Google Deutschland: antivirenProgramme	WinXP IE 6.0	1280 x 1024 True Color (32 bit) Germany Dusseldorf	00:00:11 3 Seiten Tracking
13:23:20.6700 17.08.2005	213.147.170.137 -.ycn.com (broadband) Browse http://www.google.de/search?... Google Deutschland: adaware anti spyware	WinXP Firefox 1.0	Nicht ermittelbar Nicht ermittelbar Austria Baden	00:00:00 1 Seite Tracking

Hier ist sehr gut ersichtlich, dass über jeden einzelnen Besucher sozusagen "Buch" geführt wird.

Von der Uhrzeit über die IP; das jeweilige Herkunftsland bis hin zum Betriebssystem und sogar, von welcher Webseite aus Sie gekommen sind ist alles nachvollziehbar.

Hier können wir sogar noch nach lokalen Regionen spezifizieren.

Haben Sie sich nicht auch schon einmal gefragt, warum Sie auf bestimmten Webseiten z.B. regionale DSL-Angebote passend zu Ihrem Wohnsitz eingeblendet bekommen?

Richtig, das geht auch aus Ihrer IP hervor und die aufgerufene Webseite weiß dann welches regionale Angebot sie Ihnen zeigen soll.

Es ist aber nicht illegal als Webseitenbetreiber solche Statistiken zu führen. Den allermeisten Leuten geht es dabei nicht darum Sie in Person auszuspionieren, sondern nur allgemein, das jeweilige Internetangebot für den User zu verbessern.

Nun kommen wir allerdings zu den Gefahren, die daraus resultieren.

Gefahrenquellen

Da sie nun wissen, dass es mittlerweile möglich ist, über ihre IP-Adresse an allerlei verschiedene Daten über Sie heranzukommen, sollten Sie einige Vorsichtsmaßnahmen treffen.

bisweilen haben wir dieses herausgefunden:

- die Uhrzeit Ihres Besuches
- ihrer IP-Adresse
- ihr Herkunftsland
- ihr Betriebssystem
- und von welcher Webseite sie ausgekommen sind.

Aber es sind noch weitere Daten über Sie herauszufinden. Nun kommen wir zu Informationen die etwas 'zweifelhaft' zu betrachten sind.

Über Ihren verwendeten **Browser** können nämlich noch mehr Dinge abgefragt werden. Je

nach dem welchen Browser Sie verwenden, können beinahe alle relevanten Informationen ausgelesen werden.

Dazu gehören beispielsweise:

- ob Java installiert ist
- und ob Java-Skript aktiviert ist
- ob ActiveX installiert ist
- ob Ihr Computer Cookies erlaubt
- bis hinzu ihrem Windows-Benutzernamen und Ihrer E-Mail-Adresse

wirkliche Hacker können aus diesen Informationen schnell herleiten, wo eventuelle Sicherheitslücken in ihren Systemen vorliegen. Auf diese Art können die Angreifer schnelle relevante Informationen über Ihren Computer auswerten um sie so zu attackieren.

Oftmals verwenden **Hacker** einen so genannten *Portscan* auf ganze IP-Bereiche um so einen Computer herauszufiltern der eventuelle Schwachstellen in den Sicherheitseinstellungen vorliegen hat.

Um heutzutage Opfer eines Angriffs auf dem Internet zu werden bedarf es lediglich einer online Verbindung. Gerade über die heute so beliebten Messenger wie beispielsweise ICQ oder AIM werden sehr gerne Angriffe auf fremde Computer versucht. Das dieses überhaupt funktioniert liegt daran, dass Sie bei der Installation des Messagers bereits in ihrer Firewall die Onlineverbindung des Programms erlaubt haben.

Es gibt auch komplette Webseiten im Internet wie beispielsweise Web-Seiten aus den illegalen Bereichen Warez, Apz oder auch Filesharing (P2P), die es auf sie abgesehen haben. Wenn Ihr Browser keinerlei spezielle Sicherheitseinstellungen hat, so lassen sich Java oder auch ActiveX

Doch welche Informationen hält das Internet über mich persönlich bereit?

Salopp gesagt, alles was Sie jemals in Foren, Newsgroups oder Webseiten u.s.w. geschrieben haben.

Machen Sie Sich doch einmal den Spaß und suchen bei Google nach Ihrem Vor- und Nachnamen in diesem Stil:

"Max Mustermann"

<http://www.google.de/search?hl=de&q=%22Max+Mustermann%22&meta=>

Wenn Sie nun noch den Wohnort von unserem "Max Mustermann" wissen, dann können Sie die Suchergebnisse immer weiter einengen - je mehr Informationen Sie über ihn haben, je relevanter wird das Ergebnis.

ein Zitat, was immer wieder im Internet zu lesen ist:

Es liegt in der Natur des Internets nicht vergessen zu können.

Gefahr-IP-Adresse

Betrachten wir zunächst einmal die Gefahr die sich aus ihrer IP-Adresse heraus resultiert:

Aus Sicherheitsgründen sollten Sie möglichst stündlich einmal kurz Offline gehen, das hat die Bewandnis, dass Sie von ihrem Provider, jedes Mal wenn Sie ins Internet gehen, eine neue IP-Adresse zugewiesen bekommen. Sollten Sie über mehrere Stunden hinaus immer mit derselben IP-Adresse im Internet surfen, dann ermöglichen sie es Hackern in aller Ruhe nach offenen Verbindungen (Ports) auf Ihrem Computer zu suchen. Hacker versuchen dieses mittels eines einfachen Portscanners.

Indem Sie stündlich ihrer IP-Adresse durch einmal Offline, - und dann wieder Online gehen, wechseln, machen sie es eventuellen Angreifern wie beispielsweise einem Hacker sehr schwer Sie durch Ihre IP-Adresse wieder zu finden und zu attackieren.

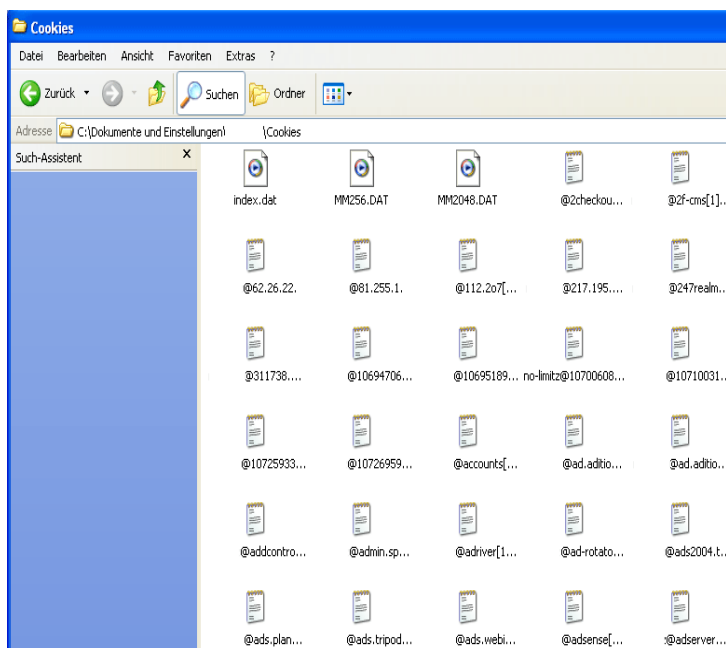
Viele Internetprovider sind heutzutage dazu übergegangen, wie beispielsweise die deutsche Telekom, nach einer Stunde eine Zwangstrennung zu vollziehen. Diese Maßnahme wurde nicht zuletzt auch aus dem Sicherheitsaspekt ins Leben gerufen.

Eine weitere Gefahr, die aus ihrer IP-Adresse resultiert, sind beispielsweise die diversen **Instand Messenger** wie **ICQ** oder **AIM**, wo nicht nur für ihre Freunde sichtbar ist und sie gerade Online sind oder nicht. Bei zu lässigen Sicherheitseinstellungen sind diese Daten im schlimmsten Falle weltweit für Jeden ersichtlich.

Was haben Cookies für eine Bedeutung?

Nun, über Cookies ist es möglich, trotz wechselnder IP's, Ihren Besuch auf einer Webseite auch immer Ihnen persönlich zuzuordnen.

Cookies sind kleine Textdateien, in denen auf Ihrem Computer abgespeichert wird wann sie zuletzt eine bestimmte Webseite besucht haben. Um sich einmal ihre Cookies näher anzuschauen öffnen Sie bitte unter:



Arbeitsplatz C:\Dokumente und Einstellungen\IHR-COMPUTERNAME\Cookies
Sollten Sie den Ordner Cookies erstmalig öffnen, so werden Sie sicherlich hoch überrascht sein wie viele dieser kleinen Textdateien sich darin verbergen.
Allerdings warnen wir an dieser Stelle davon nun sofort alle diese Dateien zu löschen.
in diesem Cookies verbergen sich allerlei Informationen. Wenn Sie z. B. sich gern in Foren oder Chats austauschen, so wird in einer dieser Dateien Ihr Benutzername und Ihr Passwort zu diesem Forum gespeichert. Auf diese Art sind Sie jedes Mal wenn Sie das Forum besuchen mit Ihren persönlichen Daten eingeloggt.
Hier wollen wir uns einmal eine dieser Textdateien (Cookies) öffnen, und sehen was dort an Informationen über uns gespeichert wurde.



in diesem Falle waren wir die Webseite Pcwelt.de besuchen. Die Webseite hat unseren Besuch registriert und einen kleinen Cookie auf unserem Computer gespeichert. In diesem Cookie ist nun vermerkt, wann wir diese Seite besucht haben und was wir uns angeschaut haben, sowie ob wir ein wiederkehrender Besucher sind. Nebenbei wurde noch vermerkt, dass unser Computer Pop-up-Werbung zulässt.

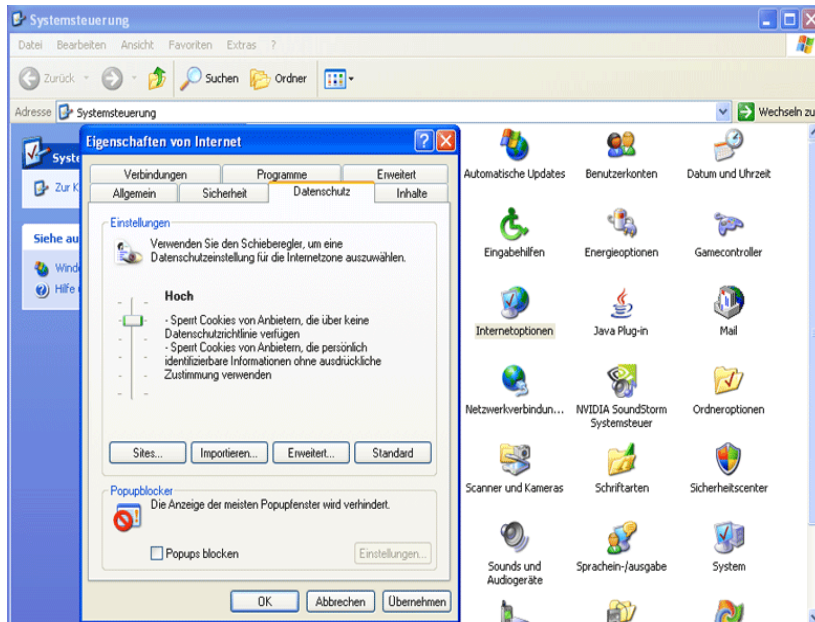
Jedes Mal wenn wir nun die Webseite pcwelt.de wieder besuchen, dann geht in der Statistik die Meldung, dass wir ein wiederkehrender Besucher sind. Nun sind wir (zumindest für Pcwelt.de) immer wieder einwandfrei zu identifizieren.

Cookies dienen also dazu, um Benutzer zielsicher zu identifizieren und den Server anzuweisen, eine benutzereigene Version einer angeforderten Webseite, Forum, Chat oder Newsgroups zu senden.

Wenn Sie sich nun einmal ihre persönlichen Cookies auf Ihrem Computer anschauen, so werden Sie sicherlich so einige Log-in Daten vorfinden. Der Großteil wird allerdings von Cookies aus der Werbewirtschaft sein. Dieses erkennt man immer sehr schnell an einschlägigen Bezeichnungen wie zum Beispiel: ADclick, Adserver, affiliate u.s.w.

wenn sie nun diesen Cookies ist einen Riegel vorschieben möchten, dann sollten Sie in Ihren Internet Optionen die Sicherheitseinstellungen etwas hoch setzen.

Dazu klicken Sie auf Start/Systemsteuerung/Internetoptionen und dort auf die Registrierkarte **Datenschutz** .



Je nach dem wie hoch Sie Ihre Datenschutzbestimmungen auswählen, werden entweder alle Cookies angenommen oder gar Keiner.

lesen Sie sich aufmerksam die verschiedensten Einstellungen unter Windows-Datenschutz durch. Sollten Sie die Einstellungen auf "keine Cookies akzeptieren" auswählen, so sollten Sie sich darüber im Klaren sein, dass sie nun auch bei keinem Forum oder Chat wo sie angemeldet sind sich automatisch einloggen können. Nun werden sie jedes Mal nach Benutzernamen und Passwort gefragt um sich einzulocken.

Immer wieder erreichen uns einige Fragen zum Thema Cookies. Diese möchten wir Ihnen hier nicht vorenthalten:

Ist es möglich dass über Cookies Viren übertragen werden können?

Weil Cookies nur Textdateien aber keine ausführbaren Programme sind, kann im Cookie selbst kein gefährlicher Code ausgeführt werden.

Zwar kann ein Virus über ein Cookie auf der Festplatte des Anwenders abgespeichert werden aber der Virus kann nicht aktiv werden. In älteren Browsern wie Netscape 2.0 und 3.0 kam es vor dass Cookies wegen eines Bugs ausgeführt wurden und dadurch ein PC zum Absturz brachten aber dass ein Cookie ein Virus enthalten kann, ist doch recht unwahrscheinlich. Sollte man ein Fan von Netscape sein sollte ein Update auf die aktuellste Version durchgeführt oder auf einen anderen Browser wie Mozilla Firefox gewechselt werden.

Können gespeicherte Informationen bei Cookies einer Person zugeordnet werden?

Wird von einem Server ein Cookie generiert wird im Normalfall kein Benutzername übertragen sondern die dort enthaltenen Daten werden nur einer IP-Adresse zugeordnet werden können.

Anders sieht es aus wenn man sich bei einem Onlineangebot wie Ebay einloggen möchte, denn dort kann ein Cookie mit seinem Benutzernamen und Passwort auf den eigenen Rechner

abgespeichert wird, damit der Login klappt. Häufig werden Cookies die einen Benutzernamen und Passwort enthalten mit SSL verschlüsselt.

Kann ein Cookie in falsche Hände gelangen?

Weil Cookies im Normalfall nicht verschlüsselt sind also im Klartext übertragen werden, ist es möglich dass diese während einer Datenübertragung von Unbekannten abgehört werden können.

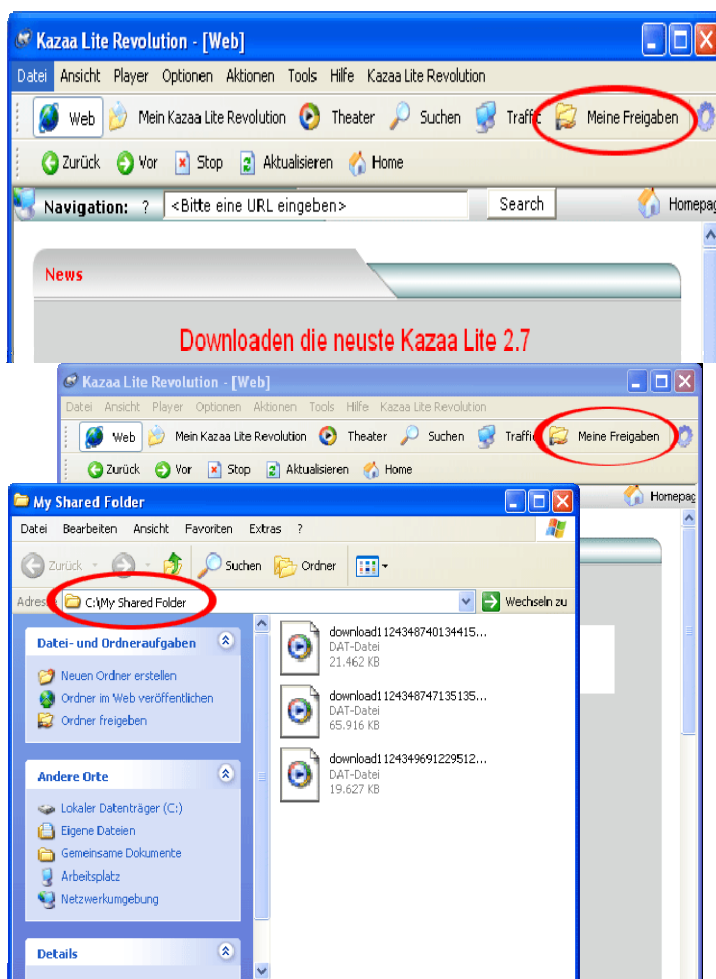
Durch DNS-Spoofing kann ein Unbekannter einen Server manipulieren was dazu führt dass ein Cookie an einen solchen Server übertragen wird obwohl das Cookie den nicht eingerichtet hat.

Dateien-freigeben

Was immer wieder zu Problemen führt sind zu offenerzige Daten freigeben bei den diversen Instand Messenger wie ICQ oder den Filesharing Programmen (P2P).

Auch hier sollten Sie sich im Klaren darüber sein, dass nun weltweit über diese verschiedenen Netzwerke auf ihre freigegebenen Daten zugegriffen werden kann. Im schlimmsten Falle werden über diese offenen Verbindungen Files wie Trojaner, Adware oder Spyware auf Ihren Computer geladen.

Überlegen Sie sich aus diesem Grunde sehr gut welchen Programmen sehr erlauben Daten von Ihrem Computer im Internet öffentlich zugänglich zu machen. Im Falle, dass sie keine Firewall installiert haben, haben sie sich auf dieser Art sehr schnell das erste posieren Tierchen eingefangen.



In den untereinander stehenden Screenshots von Kazaa können sie sehr schnell einsehen welche Dateien Sie weltweit für alle Kazaa-User zur Verfügung stellen.
Sollten Sie Kazaa installiert haben und auf die Schaltfläche "Meine Freigaben" klicken, so öffnet sich auf Ihrer Festplatte der Ordner

C: my shared Folder

Da in den diversen Filesharing Netzwerken sehr viele Viren, Würmer und Trojaner verbreitet sind liegt die Gefahr nahe, dass auch Sie sich über diese Verbreitungswege einen solchen Schädling einfangen können.

anonym-surfen-mailen

Heute ist es möglich durch Anonymisierungsdienste wie

- www.anonymizer.com
- <http://rewebber.de>

anonym durch das Netz zu surfen. Damit ein solcher Dienst genutzt werden kann besucht man seine Webseite und trägt dort dann die Webadresse ein, der man anonym einen Besuch abstatten möchte.

Bei manchen Diensten muss man sich anmelden und seine persönlichen Daten eingeben um diesen nutzen zu können aber dafür muss man diesem Dienst vertrauen, denn er könnte die eingetragenen Daten ja missbrauchen.

Muss man bei einem solchen Dienst seine persönlichen Daten hinterlegen, handelt es sich also meist nur um eine unechte Anonymität.

Neben solchen Diensten kann man mithilfe eines anonymen Proxy-Servers unbekannt durch das Netz surfen wobei dieser Proxy stellvertretend für ihren Rechner im Web auftritt und leitet alle Anfragen des Browsers ins Internet weiter.

Der große Vorteil eines Proxy-Servers ist dass die IP-Adresse des eigenen PCs vor dem Server der aufgerufenen Webseite verborgen ist. Dadurch kann der Webserver keinen Cookie auf den eigenen Rechner einspielen.

Auf der Webseite www.multiproxy.org/anon_list.html findet sich eine aktuelle Liste von Proxy-Servern.

Anonyme-Remailer

so genannten Remailer-Dienstes können Mails anonym verschickt werden. Dabei verwendet so ein Dienst die Cloaking-Technik bei der aus der Mail alle Absenderdaten entfernt und durch falsche Informationen ersetzt werden.

Die Nutzung folgenden komplett anonymen Remailer-Dienstes ist empfehlenswert.

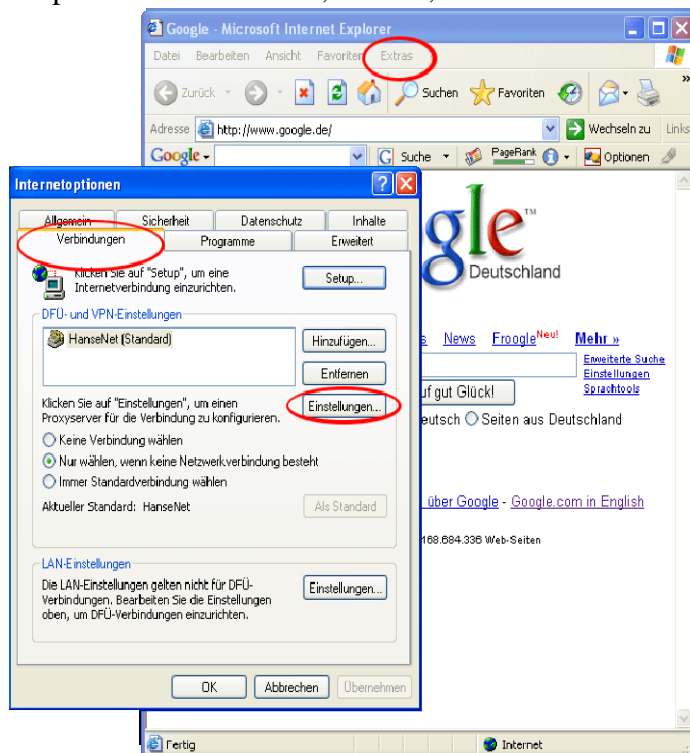
Via solche Techniken haben wir schon des öfteren E-Mails mit dem Absender des Bundestags, oder des Oval-Office u.s.w. als Scherz bekommen.

anonymen-Proxy-einrichten

Soll nur ein Dienst über den Port möglich sein, wird auf dem Applikation Server eine Software aktiv, die das Paket von einer Netzwerkseite auf die andere Netzwerkseite überträgt, ein so genannter Proxy.

Aus Sicht des zugreifenden Benutzers sieht es so aus, als würde er mit dem eigentlichen Server-Prozess des Dienstes auf einem Zielrechner kommunizieren. Tatsächlich kommuniziert der Benutzer aber mit dem Proxy (einem Stellvertreter), der nach beiden Seiten als Vermittler auftritt, so dass niemals eine Verbindung zwischen Zielrechner und Besucher zustande kommt. Jeder Proxy auf dem Applikation Gateway kann speziell für den Dienst, für den er zuständig ist, weitere Sicherheitsdienste anbieten. Bedingt durch den jeweiligen speziellen Proxy und das Wissen um den Kontext eines speziellen Dienstes ergeben sich im Applikation Gateway umfangreiche Sicherungs- und Protokollierungsmöglichkeiten.

Entsprechend der Vielzahl der angebotenen Dienste gibt es anwendungsspezifische Gateways beispielsweise für Telnet, E-Mail, HTTP u.a.

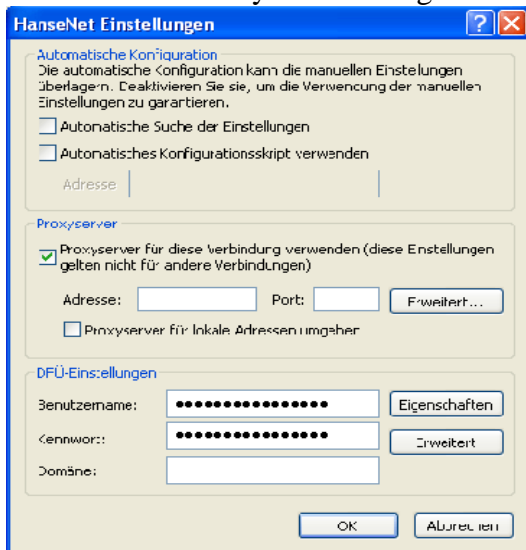


Damit der Browser MS Internet Explorer mit einem anonymen Proxy-Server arbeiten kann, muss dieser konfiguriert werden.

Starten Sie den Browser und klicken in der Menüleiste auf Extras sowie dann auf Internetoptionen.

Anschließend wird auf den Reiter Verbindungen geklickt und eine Verbindung ausgewählt gefolgt von einem Klick auf den Punkt Einstellungen. Nun wird ein Häkchen beim Kästchen „Proxyserver für diese Verbindung verwenden“ gemacht und dort die IP-Adresse des anonymen Proxy-Servers inklusive Server-Port eingetragen, welche Sie aus einer Proxy-Liste ausgewählt haben. Als letztes wird auf den Button OK geklickt und damit die Änderungen aktiviert.

Wenn der eingetragene Proxy-Server nicht funktionieren sollte, wählen Sie von einer Liste einen anderen Proxy aus und tragen diesen ein.



Als letzter Schritt wird eine Onlineverbindung hergestellt und die Eingabeaufforderung über Start/Programme/Zubehör ausgewählt und der Befehl ping inkl. der IP-Nummer des Proxy-Servers eingegeben. Wenn dieser Server antwortet kann die Webadresse in den Browser eingetragen werden.

Weil Proxy-Server nur temporär verfügbar sind, sollte er regelmäßig gewechselt werden damit man im Netz wieder anonym unterwegs sein kann.

Anonym-Peekabooty

Im Jahre 2001 entwickelte die bekannte Hackergruppe „Cult of the dead Cow“ oder kurz cDc den speziellen Browser **Peekabooty** mit dem man sich anonym und freier im Internet bewegen kann. Wird der Browser auf dem Rechner installiert, stellt er eine Verbindung zum Peekabooty-Netz, der als zentraler Proxy funktioniert.

Weil die Datenübertragung zwischen Server und Browser verschlüsselt wird, ist es damit auch möglich Firewalls zu umgehen.

In Ländern wo das Internet verboten ist oder stark eingeschränkt wurde bedeutet dieser Browser eine neue Freiheit aber den Peekabooty-Proxy kann man auch nutzen indem die Adresse eines solchen Proxys einträgt.

Jedoch hat Peekabooty einen Nachteil weil er erst am Anfang seiner Entwicklung steht und nur wenige Peekabooty-Knoten zu finden sind aber je mehr Anwender die Technologie des Browsers verwenden umso höher wird die Zahl der Peekabooty-Proxys werden.

Der Browser ist als Open Source Software programmiert und steht öffentlich unter der GNU General Public Licence (GNU-GPL) auf der Webseite <http://sourceforge.net> kostenlos zum Download bereit und wird ständig von den Anwendern weiterentwickelt.

In unseren Ländern eigentlich nicht nötig um an Informationen im Web zu kommen doch gibt es auch Länder, in denen gerade dieser Informationsfluss gern unterbunden gesehen würde.

Wir möchten hier aber nicht näher darauf eingehen um welche Länder es sich handelt.

Nutzwerk.de

Nutzwerk.de

Diese Firma wurde 1997 gegründet und hat ihren Service bis heute unter Saversurf.com in 70 Länder und in allen fünf Erdteilen etabliert.

Nutzwerk hat mit den Geschäftsführern Ramona Wonneberger und René Holzer Basistechnologien für das Internet im Bereich "**anonym surfen**" geschaffen. die Unternehmensziele von Nutzwerk sind es, Probleme und Aufgaben des Internets zentral zu lösen ohne dass ein User Software installieren und pflegen muss.

1998 wurde von der Firma Nutzwerk.de ein Echtzeit-Datenfilter erfunden, der Datenströme inhaltlich analysiert und auswertet. dieser Datenfelder ist auch in Deutschland patentiert (Nummer DE 10048113). Diese Nutzwerklösungen basieren auf standardisierten Protokollen und Diensten des Internets und werden dem Nutzer systemunabhängig angeboten.

Zu den Aufgaben von Nutzwerk`s Datenfilter gehören in Echtzeit folgende Filterprotokolle:

- kritische Dateien, wie Viren
- 0190-Dialer
- Werbung (Spyware)

Filterung und Vernichtung. dieser Dienst ist so konzipiert, ohne dass auf dem Anwender-Computer eine Software installiert werden muss. Des Weiteren überprüft der Datenfilter von Nutzwerk auch ausgehende Daten, damit verhindert wird, dass unwissentlich eine E-Mail verschickt werden kann, die beispielsweise einen Virus enthält.

Seit dem Jahr 2002 bietet Nutzwerk auch für Privat-Personen zwei SaferSurf Dienstleistungen an:

ein Komplettschutz-Paket für Internet und E-Mail sowie Paket für schnelleres und billigeres Surfen.

Mit dem Echtzeit Datenfilter war Nutzwerk Testsieger für diesen Service und hat beim MDR Fernsehen Sicherheitslösungen von AOL und T-Online auf die Plätze verwiesen.(Ausgabe 04/2003 bei Computerbild).

Mittlerweile hat der Dienst von Nutzwerk.de sogar das **TÜV Siegel** erhalten und den Leipziger Innovationspreis für das Internet gewonnen.

Mittlerweile hat Nutzwerk auch Speziallösung wie SaferSurf-School in Schulen und Bibliotheken in Sachsen und Sachsen-Anhalt erfolgreich eingesetzt.

Nutzwerk sieht seine Kompetenzen als Forschungs- und Technologieunternehmen. Eigenständige Technologien sind weltweit zum Patent angemeldet.

Speichert SaferSurf personenbezogene Daten?

Zitat:

"Niemand, auch keine Bundesbehörde mit einem richterlichen Beschluss, kann uns zwingen Ihre Daten herauszugeben. SaferSurf ist einerseits durch seinen Status als Diensteanbieter durch das Gesetz geschützt und zum anderen speichern wir Ihre IP-Adresse nicht gemeinsam mit Nutzungsdaten. Damit kann SaferSurf oder ein Dritter zu keinem Zeitpunkt eine Verknüpfung mit angewählten Inhalten herstellen."

Dieser Aussage von Nutzwerk haben wir nichts hinzuzufügen. Alles in Allem ein rundum gelungener Dienst, der nicht "nur" im Internet anonymisiert, sondern nebenbei auch noch vor Bedrohungen vielfältigster Art schützt.

Weitere Informationen zum Thema **anonym surfen** erhalten Sie auf:

[Nutzwerk.de](https://nutzwerk.de)